Dc3 Digital Forensics Challenge

104 – Signature Analysis

Team Information

Team Name: ____

Results Email: ____

Examination Time Frame: to

Instructions

Description: Examine the files in the **104_Signature_Analysis_Challenge2008** folder to determine which files are using the proper signature information and filename display and which are not. Report the full filename for mismatched files, a detailed explanation of your process (software or technique) used to examine and determine your results, and provide the corrected file.

Points will be awarded for each successfully identified signature mismatch and reasoning for your decision.

Total Weighted Points: **10 Total Points available per entry – Total 100 Points Available**

1. **Answers –** Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer: Points Awarded:

Date: Review Period: to

Completed: □ Yes □ No □ Partial

REPORT OF EXAMINATION

<Example Area>

File Name:	Signature Good	Bad	Correct Signature
Example.exe	**X**		**Example.exe**
Challenge.doc		**X**	**Challenge.com**

Located by using .... and or process of .... Research revealed ....

<Answer Area>

File Name:

Identified Good or Bad by using .... and or process of .... Research revealed ....

Please attach additional sheets as needed.

Page ______ of ______ Initials ________________

METHODOLOGY / NOTES FORM

Tool Information

Type	**Name**	**Publisher**
Commercial / Open Source		

Site:

Type	**Name**	**Publisher**
Commercial / Open Source		

Site:

Type	**Name**	**Publisher**
Commercial / Open Source		

Site:

Date/Time	Notes

Report of Examination

File Name	Signature Good	Bad	Correct Signature
1. 245.JPG	X		
File Name	Signature Good	Bad	Correct Signature
2. 249.JPG	X		
File Name	Signature Good	Bad	Correct Signature
3. 255.JPG	X		
File Name	Signature Good	Bad	Correct Signature
4. AutoWire.bmp	X		
File Name	Signature Good	Bad	Correct Signature
5. blank.jpg		X	.asp

Identified bad signature using the following software:

Guidance Software’s EnCase v 5.05J
AccessData’s Forensic Tool Kit 1.8

Researched the \x3C \x25 \x40 \x20 \x20 \x43 (<%@ CO) file signature and found several references to the .asp file extension. I continued to research the content of the file and found that my initial findings of the “asp” file extension were correct.

File Name	Signature Good	Bad	Correct Signature
6. blue.bmp		X	.asp

Identified bad signature using the following software:

Guidance Software’s EnCase v 5.05J
AccessData’s Forensic Tool Kit 1.8

Researched the \x3C \x25 \x40 \x20 \x20 \x43 (<%@ CO) file signature and found several references to the .asp file extension. I continued to research the content of the file and found that my initial findings of the “asp” file extension were correct.

File Name	Signature Good	Bad	Correct Signature

7.Bluestar.gif	X		

File Name	Signature Good	Bad	Correct Signature
8. Chaff_Floral_1197.bmp	X		

File Name	Signature Good	Bad	Correct Signature
9. Chaff_Landscape_158.gif	X		

File Name	Signature Good	Bad	Correct Signature
10. Chaff_Landscape_161.gif	X		

File Name	Signature Good	Bad	Correct Signature
11 CLOCK.MOV		X	.cab

Identified bad signature using the following software:

Guidance Software's EnCase v 5.05J
AccessData's Forensic Tool Kit 1.8

Researched the \x4D \x53 \x43 \x46 (MSCF) file header and found several references to potential file extensions including .CAB (Microsoft Cabinet File), .PPZ (PowerPoint Packaged Viewer), .SNP (Microsoft Access Snapshot Viewer. I then tested each extension and my results were that the proper file extension is the ".CAB" extension.

File Name	Signature Good	Bad	Correct Signature
12. DollL Sales Worldwide.html		X	.JPG

Identified bad signature using the following software:

Guidance Software's EnCase v 5.05J
AccessData's Forensic Tool Kit 1.8

I researched the \xFF \xD8 \XFF \xE0 file header and found references to the .JPG file extension.

File Name	Signature Good	Bad	Correct Signature
13. intro.mpeg		X	.zip

Identified bad signature using the following software:
Guidance Software's EnCase v 5.05J
AccessData's Forensic Tool Kit 1.8

I researched the \x50 \x4B (PK) file header and found references to the .ZIP file extension. I tested this file extension in both a forensic environment using EnCase 5.05J and in a Microsoft Windows XP environment. The results were as expected, the zip file opened and revealed picture files.

File Name	Signature Good	Bad	Correct Signature
14. ipp_0004.asp	X		

File Name	Signature Good	Bad	Correct Signature
15. pctools.zip		X	.cat

Identified bad signature using the following software:
Guidance Software's EnCase v 5.05J
AccessData's Forensic Tool Kit 1.8

I researched the \x30 \x82 \x21 (0,!) file header and didn't find any references any extensions. I searched the contents of the file for any unique identifiable strings. I located several references to Microsoft and Verisign. I continued to search and found "\x50 \x43 \x41 \x30 \x1E \x17 \x0D \x30 \x32 \x31\x32 \x31 \x39 \x31 \x38 \x30 \x31 \x31 \x37 5A" (PCA0··021219180117Z). I searched what I felt was a unique search string and reviewed a file with the same string which was a Security Catalog Information file or ".Cat" extension. I tested this file extension in both a forensic environment using EnCase 5.05J and in a virtual Microsoft Windows XP environment. The results were as expected, the .cat file opened and revealed a Security Catalog Information file.

File Name	Signature Good	Bad	Correct Signature
16. SAILBOAT.JPG		X	CHM

I researched the \x49 \x54 \x53 \x46 (ITSF) file header and found references to the .CHM file extension. I tested this file extension in both a forensic environment using EnCase 5.05J and in a virtual Microsoft Windows XP environment. The results were as expected; the .CHM file opened and revealed a Microsoft HTML Help compiled help file.

File Name	Signature Good	Bad	Correct Signature
17. Straightline.tif		X	ASP

Identified bad signature using the following software:

Guidance Software's EnCase v 5.05J
AccessData's Forensic Tool Kit 1.8

Researched the \x3C \x25 \x40 \x20 \x20 \x43 (<%@ CO) file signature and found several references to the .asp file extension. I continued to research the content of the file and found that my initial findings of the "asp" file extension were correct.

File Name	Signature Good	Bad	Correct Signature
18. SYSTEM.1ST		X	.DAT

Identified bad signature using the following software:

Guidance Software's EnCase v 5.05J
AccessData's Forensic Tool Kit 1.8

Researched the \x43 \x52 \x45 \x47 (CREG) file signature and found several references to the .dat file extension. I continued to research the content of the file and found that my initial findings of the "dat" file extension were correct.

File Name	Signature Good	Bad	Correct Signature
19. SYSTEM.CB	X		

File Name	Signature Good	Bad	Correct Signature
20. Windows.wav		X	.Cnt

Identified bad signature using the following software:

Guidance Software’s EnCase v 5.05J
AccessData’s Forensic Tool Kit 1.8

Researched the \x3A \x42 \x61 \x73 (:Base) file signature and found several references to the .cnt file extension. I continued research and identified a unique identifiable string “1 This file is not meant for browsing=WIN_HELP_AUTOCLOSE”. I searched what I felt was a unique search string and reviewed several references to files with the .cnt extension.